(19) Europäisches Patentamt
European Patent Office
Office uropé n d s brevets

(11) EP 0 813 325 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
17.12.1997 Bulletin 1997/51

(51) Int. Cl.[6]: **H04L 29/06**

(21) Application number: **97109412.3**

(22) Date of filing: **10.06.1997**

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **12.06.1996 US 664019**

(71) Applicant: **AT&T Corp.**
New York, NY 10013-2412 (US)

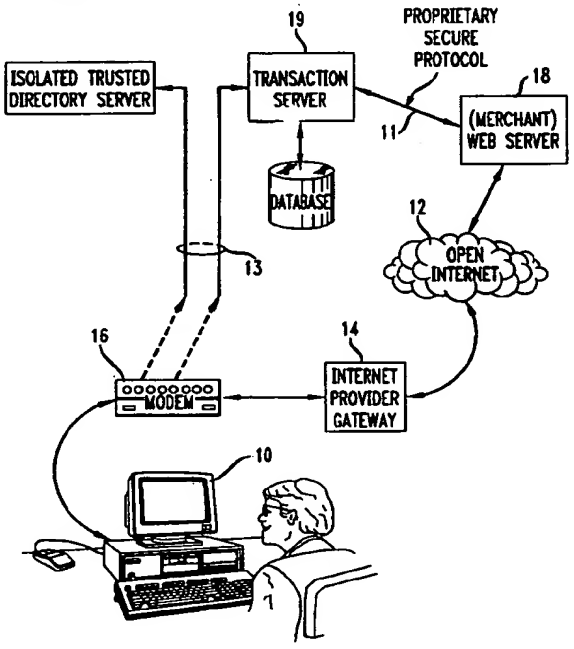
(72) Inventor: **Apte, Jitendra**
Woodbridge, NJ 07095 (US)

(74) Representative:
KUHNEN, WACKER & PARTNER
Alois-Steinecker-Strasse 22
85354 Freising (DE)

(54) A mechanism for enabling secure electronic transactions on the open internet

(57) A method is provided for performing a transaction that is initiated over an open communication network between a user and a remotely located server. The open communication network may be the Internet, for example. In accordance with one embodiment of the method, a transaction identification number is received from the remotely located server over the open network and subsequently, communication between the user and the remotely located server is discontinued. Communication is established between the user and a transaction server. The transaction server is operatively coupled to the user and the remotely located server over a communication network which is isolated from the open network. The transaction identification number is transmitted to the transaction server over the communication network. After the transaction server confirms the validity of the transaction identification number, in response to a request from the transaction server, a transaction authorization number is transmitted over the communication network to the transaction server to complete the transaction.

FIG. 1



EP 0 813 325 A2

BNSDOCID: <EP___0813325A2_I_>

Description

Field of the Invention

This invention relates generally to a method for performing secure transactions on open communication networks and, in particular, to a method and apparatus for performing transactions such as purchases over the World Wide Web.

Background of the Invention

Open public networks such as the Internet, and in particular the World Wide Web, have undergone tremendous growth as a distribution channel for businesses. These businesses typically provide an Internet site to promote one or more products or services. Of course, it would be convenient if customers could actually complete a transaction and purchase a product or service over the Internet. However, it is currently difficult to secure data traffic that traverses the Internet because the Internet is an open environment with no guarantees of data privacy and thus a third party can access or alter the data as it is in transit. Consequently sensitive data such as credit card numbers cannot be transmitted over the Internet with adequate assurances of security.

A variety of techniques have been explored to secure data on the Internet. Many of these techniques involve data encryption, which may provide adequate security for a limited time. However, encryption techniques are continuously in jeopardy of being broken because technologies to break encryption schemes are being developed as rapidly as the encryption techniques themselves and because the computing power and communication systems needed for decryption are fast becoming ubiquitous and cheap. Moreover, in addition to the technological problems of providing security on the Internet, there is a large socio-cultural impediment to performing electronic transactions on the Internet simply because people question its security. Accordingly, it would be desirable to provide a convenient method for performing a reasonably secure transaction over the Internet.

Summary of the Invention

The present invention provides a method for performing a transaction that is initiated over an open communication network between a user and a remotely located server. The open communication network may be the Internet, for example. In accordance with one embodiment of the method, a transaction identification number is received from the remotely located server over the open network and subsequently, communication between the user and the remotely located server is discontinued. Communication is established between the user and a transaction server. The transaction server is operatively coupled to the user and the remotely located server over a communication network which is isolated from the open network. The transaction identification number is transmitted to the transaction server over the communication network. After confirming the validity of the transaction identification number, the transaction server requests a transaction authorization number. In response to this request, a transaction authorization number is transmitted over the communication network to the transaction server to complete the transaction.

The transition in communication between the remotely located server and the transaction server may occur automatically upon a request from the user to complete the transaction. Accordingly, the user can perform a secure transaction in an extremely convenient manner.

Brief Description of the Drawings

FIG. 1 shows an example of a system constructed in accordance with the present invention which is incorporated into the World Wide Web.

FIG. 2 shows a flow diagram illustrating one embodiment of the process used to purchase an item from the World Wide Web in accordance with the present invention.

Detailed Description

The present invention allows an individual to browse the open World Wide Web (WWW) and in a seamless manner perform secure transactions over a secure electronic communication medium that is isolated from the WWW. Such secure communications media are often employed by banks, for example, to allow customers to perform home banking over a personal computer. These secure communication media typically employ an encrypted proprietary protocol operating over a telephone link (i.e., a circuit switched POTS connection). FIG. 1 shows an example of a system in accordance with the present invention which is incorporated into the WWW.

A personal computer 10 or other data processing device is coupled to the open Internet 12, and in particular the WWW, via an Internet provider gateway 14. The computer 10 interfaces with the gateway 14 via an input/output device 16 that typically includes a modem. The computer 10 may be employed by a user to search the WWW with a web browser in a conventional manner and communicate with a remotely located server 18 that may represent, for example, a vendor advertising a product or service. Examples of web browsers include Netscape's Navigator and Microsoft's Internet Explorer, for example.

Currently, if the user desires to purchase the product or service from the vendor, the user provides a credit card number over the network, thus potentially allowing a third party access to the card number, even if an encryption technique is employed. In accordance with the present invention, however, this problem is avoided

BNSDOCID: <EP___0813325A2_I_>

because sensitive data is never transmitted over the open WWW. Rather, in response to the user's request to make a purchase, the vendor 18 transmits a purchase order number both to the user 10 over the WWW and to a transaction server 19 that is isolated from the Internet. The vendor 18 communicates with the transaction server 19 over any desired communication system 11 that is isolated from the Internet. This system 11 may employ a proprietary protocol that operates over a telephone link such as any of those conventionally used for banking.

The user subsequently pays for the purchase by initiating communication between the computer 10 and the transaction server 19 over another communication system 13 that is isolated from the WWW and which also may employ a proprietary protocol operating over a telephone link. The user provides the purchase order number to the transaction server 19 and proceeds to complete the purchase by providing a credit number. Since the transaction server 19 is isolated from the open WWW the inherent risks of communicating sensitive information is avoided. The transaction between the user and the transaction server has a degree of security at least equivalent to the security provided by a conventional telephone and preferably to the level of security provided by proprietary home banking, tax filing, or bill paying communication systems. A system employing a proprietary protocol to transmit data over the telephone system is advantageous because consumers by and large believe that transmitting sensitive data in this manner (by speaking or faxing the data, for example) is secure. Support for this belief is provided by the success of on-line banking, tax filing and bill paying systems.

It should be noted that the term "isolated" as used herein refers to isolation with respect to information transport and not physical isolation. For example, portions of the communications system 13 and the Internet 12 may share the same physical links such as the user's local telephone line. However, the communication system 13 and the Internet 12 do not communicate with one another.

In accordance with one aspect of the invention, the user is provided with software to be executed on the computer 10 which automatically performs the transition in communication from the WWW 12 to the transaction server 19 so that the details involved are invisible to the user. That is, when the user wishes to place an order, there is no need to manually disconnect from the WWW 12 and initiate communication with the transaction server 19 over the isolated communication system. Rather, the software residing in the computer 10 performs the transaction so that the user may even be unaware that the computer 10 has disconnected from the WWW and initiated communication with another network.

FIG. 2 shows a flow diagram illustrating one embodiment of the process used to purchase an item from the WWW in accordance with the present invention. Each block in FIG. 2 identifies the operations to be performed by the personal computer to provide the functionality contemplated by the present invention. It should be noted that the operations performed by the computer may be implemented programically by software residing on the computer or by direct electrical connections through customized integrated circuits or by a combination of both.

The process begins in step 200, in which communication is established between the computer and the WWW in a conventional manner. The user browses public sites on the WWW and ultimately decides to purchase a product or service from a vendor. The user's computer receives the purchase order number in step 209 of FIG. 2. The vendor generates a purchase order number in response to the user's request and transmits the order number to both the transaction server and the user's computer 10. The vendor directs the user to contact the appropriate transaction server and may additionally provide the user with the server's telephone number. which may, for example, be an 800 number. The telephone number may be unique to the particular transaction server or it may be unique to both the transaction server and the vendor (so that each transaction server can receive requests in connection with different vendors each having a unique telephone number). Moreover, the present invention contemplates the provision of a plurality of transaction servers as demand warrants and in some cases vendors may work in cooperation with more than one transaction server.

In step 201 communication between the WWW and the computer is suspended by either discontinuing the communication session or by placing the connection to the WWW in a hold state via a three-way calling service. In step 203 the computer establishes communication with the transaction server over the secure network. As previously noted, the vendor may provide the user with the appropriate telephone number. This may be accomplished in a simple manner by having the vendor display the telephone number on its web page. However, this scheme may not be sufficiently secure because a third party could potentially alter the telephone number while it is being transmitted from the server to the user, thereby fraudulently obtaining the user's credit card number by having the user call a telephone number accessible to the third party.

In yet another alternative embodiment of the invention, the telephone number of the transaction server may be locally stored in the computer or, alternatively, the user may retrieve the appropriate telephone number from a directory located in the secure communication system which includes the transaction server. The telephone number of the directory may be stored in the computer or it may be provided by the vendor. The directory may reside on the transaction server itself or it may reside in another component in communication with the secure system. In one particular embodiment of the invention, the computer first uses the Universal Resource Locator (URL) of the vendor and attempts to

BNSDOCID: <EP___0813325A2_I_>

retrieve the phone number for its transaction server from a locally stored directory. If the number is not found, the computer automatically dials the directory located on the secure network and downloads the appropriate telephone number. If the telephone number is still not found, the computer prompts the user to provide the appropriate number. Finally, if the number is unavailable, the attempted transaction is aborted and the computer returns to vendor's site on the WWW, which had been on hold. In this situation customer service should be called.

Returning to step 203, after communication has been established with the transaction server, the user provides the server with the purchase order number in step 202. The transaction server locates the purchase order and may echo to the user a list of the products or services to be purchased. The user approves the purchase and in step 204 provides a credit card number to complete the transaction. Once the transaction between the computer and the transaction server is complete, the computer ends the communication session with the transaction server in step 205 and resumes communication with the WWW in step 207. The transaction server subsequently transmits the completed order back to the vendor or directly to a shipping department.

In one embodiment of the invention, the communication session between the computer 10 and the transaction server is configured to appear to the user as a WWW communication session. That is, the interface between the computer 10 and the transaction server is designed to function in a format similar to a WWW browser so that the user is virtually unaware that the computer has suspended communication on the WWW and initiated communication over a secure network isolated from the WWW. From the user's perspective this advantageously simplifies the task of purchasing an item over the WWW in a relatively secure manner.

In accordance with one aspect of the invention, the purchase order number provided to the user may be randomly generated by the vendor's server. This feature prevents unauthorized users from dialing in to the transaction server and attempting to access orders by trying arbitrary purchase order numbers. Additionally, the transaction server can limit the user to a predetermined number (e.g. three) of incorrect order numbers before terminating the connection.

In the embodiment of the invention discussed in connection with FIG. 2, the user's computer 10 initiated contact with the transaction server, as opposed to the transaction server initiating contact with the user. While the present invention encompasses both procedures, the former procedure is advantageous because if the latter procedure is used, an unauthorized party on the open Internet could detect a message from the user to the vendor requesting a return call for credit card authorization. This party could then call the user, thus emulating the transaction server to fraudulently acquire the user's credit card number.

It will be appreciated that those skilled in the art will be able to devise numerous arrangements which, although not explicitly shown or described herein, embody the principles of the invention. Accordingly, all such alternatives, modifications and variations which fall within the spirit and broad scope of the appended claims will be embraced by the principles of the invention. For example, while the invention has been described in connection with FIGS. 1 and 2 as a method for completing a transaction on the Internet, the invention is more broadly applicable to a method for completing a transaction on other open communication systems as well.

Claims

1. A method for performing a transaction initiated over an open communication network between a user and a remotely located server, comprising the steps of:

   a. receiving a transaction identification number from the remotely located server over the open network;
   b. discontinuing communication between said user and said remotely located server;
   c. establishing communication between said user and a transaction server, said transaction server being operatively coupled to said user and said remotely located server over a communication network isolated from said open network;
   d. transmitting said transaction identification number to said transaction server over said communication network;
   e. after the transaction server confirms validity of the transaction identification number, transmitting over said communication network, in response to a request from said transaction server, a transaction authorization number to said transaction server to complete the transaction.

2. The method of claim 1 wherein steps (b) and (c) occur automatically in response to a request from said user to complete the transaction.

3. The method of claim 2 wherein steps (b) and (c) occur in a manner substantially transparent to said user.

4. The method of claim 1 wherein communication over said communication network between said user and said transaction server employs an encrypted protocol at least in part operating over a telephone link.

5. The method of claim 1 wherein said open network comprises the Internet.

BNSDOCID: <EP___0813325A2_I_>

6. The method of claim 5 wherein said open network comprises the world wide web.

7. The method of claim 1 wherein said user is in communication with said remotely located server and said transaction server over a personal computer.

8. The method of claim 1 wherein said remotely located server is employed by a vendor to advertise on the open network.

9. The method of claim 8 wherein said transaction comprises a purchase.

10. The method of claim 9 wherein said transaction authorization number is a credit card number.

11. The method of claim 1 wherein step (a) further comprises the step of receiving from said remotely located server a telephone number of said transaction server.

12. The method of claim 1 wherein step (b) includes the step of suspending communication between said user and said remotely located server by placing said remotely located server in a hold state.

13. The method of claim 1 wherein said communication in step (c) is initiated by said user.

14. The method of claim 13 wherein said user initiates communication with said transaction server by performing the step of retrieving a locally stored telephone number of said transaction server.

15. The method of claim 13 wherein said user initiates communication with said transaction server by retrieving a telephone number from a directory located in said communication network.

16. The method of claim 6 wherein said transaction is initiated by the user using a World Wide Web browser

17. The method of claim 1 further comprising the steps of:

f. discontinuing communication between said user and transaction server;
g. subsequently resuming communication between said user and said remotely located server.

18. The method of claim 17 wherein steps (f) and (g) occur automatically after completion of step (e).

19. A computer readable medium having a computer program encoded thereon for performing a transaction initiated over an open communication network between a user and a remotely located server, comprising:

a first portion of said medium having a first program segment for receiving a transaction identification number from the remotely located server over the open network;
a second portion of said medium having a second program segment for discontinuing communication between said user and said remotely located server;
a third portion of said medium having a third program segment for establishing communication between said user and a transaction server over a communication network isolated from said open network;
a fourth portion of said medium having a fourth program segment for transmitting said transaction identification number to said transaction server over said communication network;
a fifth portion of said medium having a fifth program segment for transmitting over said communication network, after the transaction server confirms validity of the transaction identification number and in response to a request from said transaction server, a transaction authorization number to said transaction server to complete the transaction.

20. The medium of claim 19 wherein said second and third program segments are automatically executed in response to a request from said user to complete the transaction.

21. The medium of claim 20 wherein said second and third program segments are executed in a manner substantially transparent to said user.

22. The medium of claim 19 wherein said third, fourth, and fifth program segments employ an encrypted protocol operating at least in part over a telephone link.

23. The medium of claim 19 wherein said open network comprises the Internet.

24. The medium of claim 23 wherein said open network comprises the World Wide Web.

25. The medium of claim 19 wherein said remotely located server is employed by a vendor to advertise on the open network.

26. The medium of claim 25 wherein said transaction comprises a purchase.

27. The medium of claim 26 wherein said transaction authorization number is a credit card number.

BNSDOCID: <EP___0813325A2_I_>

28. The medium of claim 19 wherein said first program segment further receives from said remotely located server a telephone number of said transaction server.

29. The medium of claim 19 wherein said second program segment suspends communication between said user and said remotely located server by placing said remotely located server in a hold state.

30. The medium of claim 19 wherein said third program segment initiates communication between said user and said transaction server.

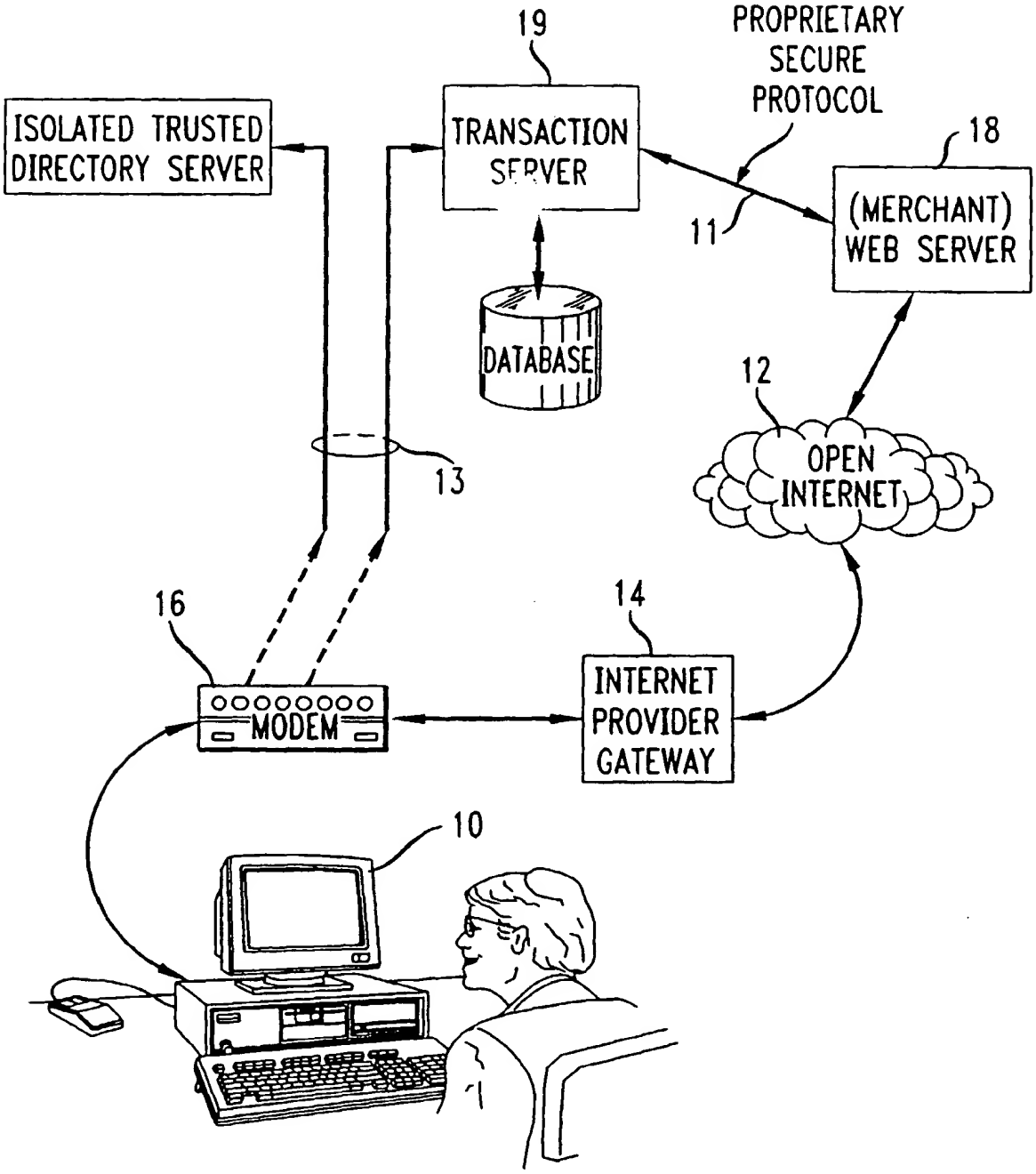
31. The medium of claim 30 wherein said third program segment initiates communication with said transaction server by retrieving a locally stored telephone number of said transaction server from a sixth portion of said medium.

32. The medium of claim 30 wherein said third program segment initiates communication with said transaction server by retrieving a telephone number from a directory located in said communication network.

33. The medium of claim 24 further comprising a sixth portion of said medium having a sixth program segment for browsing on the World Wide Web.

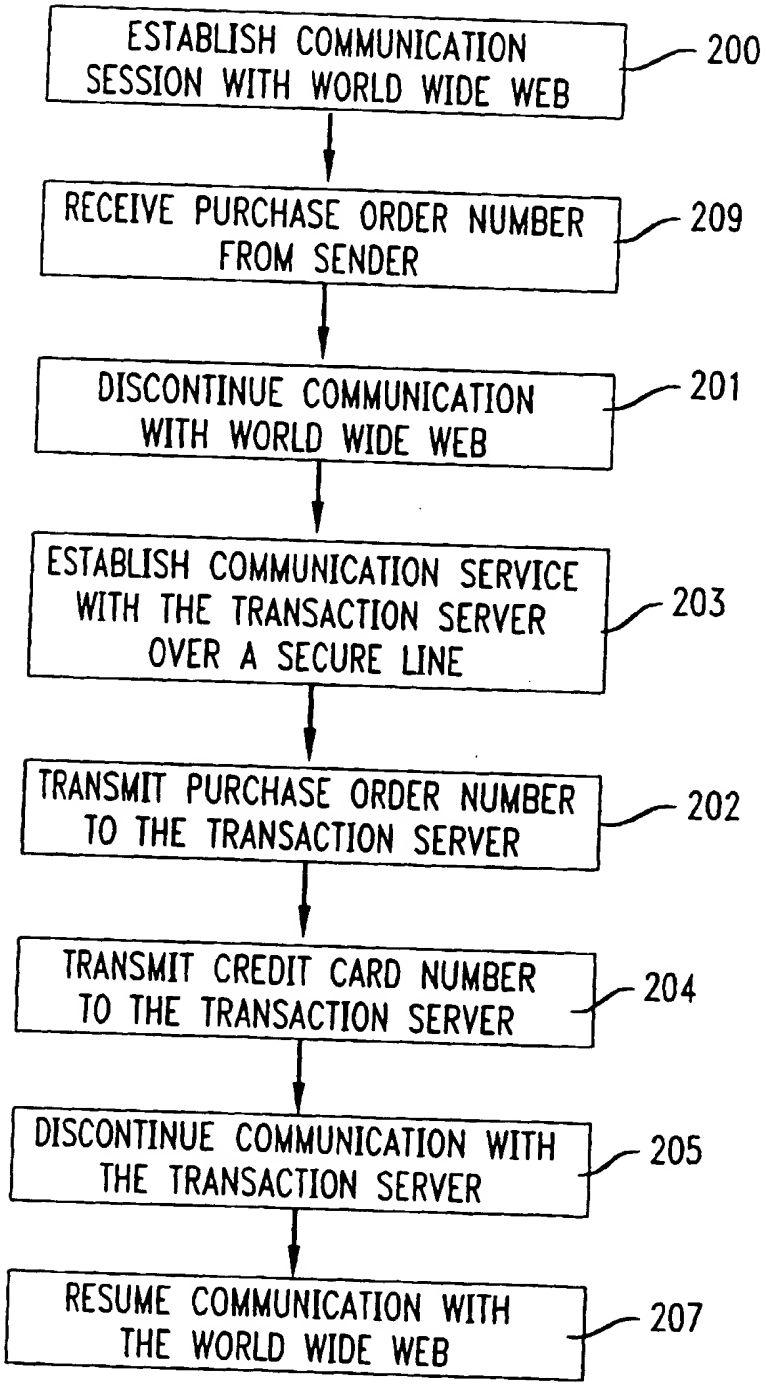
BNSDOCID: <EP___0813325A2_I_>

FIG. 1



BNSDOCID: <EP___0813325A2_I_>

FIG. 2



BNSDOCID: <EP___0813325A2_I_>

(19) Eur päisches Patentamt
European Patent Office
Office européen d s brevets

(11) EP 0 813 325 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
30.08.2000 Bulletin 2000/35

(43) Date of publication A2:
17.12.1997 Bulletin 1997/51

(21) Application number: **97109412.3**

(22) Date of filing: **10.06.1997**

(51) Int. Cl.[7]: **H04L 29/06**, G06F 17/60, G07F 19/00

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: **12.06.1996 US 664019**

(71) Applicant: **AT&T Corp.**
New York, NY 10013-2412 (US)

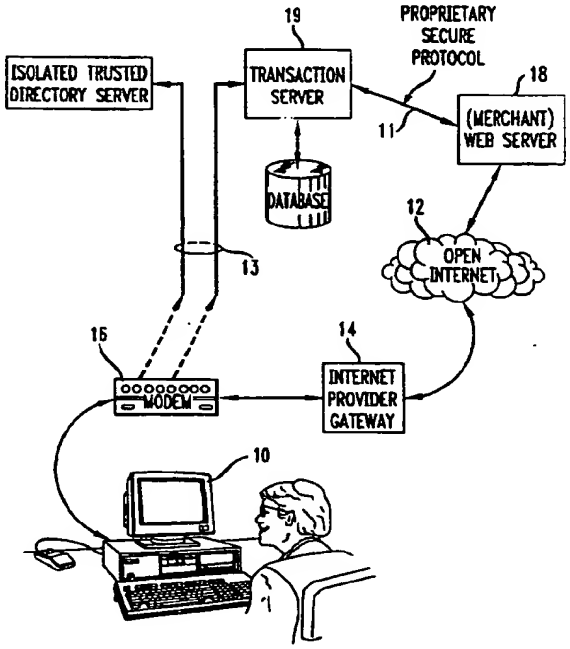
(72) Inventor: **Apte, Jitendra**
Woodbridge, NJ 07095 (US)

(74) Representative: **Kuhnen & Wacker**
Patentanwaltsgesellschaft mbH,
Alois-Steinecker-Strasse 22
85354 Freising (DE)

(54) A mechanism for enabling secure electronic transactions on the open internet

(57) A method is provided for performing a transaction that is initiated over an open communication network between a user (10) and a remotely located server (18). The open communication network may be the Internet (12), for example. In accordance with one embodiment of the method, a transaction identification number is received from the remotely located server (209) over the open network and subsequently, communication between the user and the remotely located server is discontinued (201). Communication is established between the user and a transaction server (203). The transaction server is operatively coupled to the user and the remotely located server over a communication network which is isolated from the open network. The transaction identification number is transmitted to the transaction server over the communication network (202). After the transaction server confirms the validity of the transaction identification number, in response to a request from the transaction server, a transaction authorization number is transmitted over the communication network to the transaction server to complete the transaction.

FIG. 1



EP 0 813 325 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 10 9412

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 590 861 A (AMERICAN TELEPHONE & TELEGRAPH) 6 April 1994 (1994-04-06) * column 1, line 9 - line 24 * * column 3, line 15 - line 17 * * column 3, line 43 - column 4, line 7 *	1-33	H04L29/06 G06F17/60 G07F19/00
A	BAGSHAW E: "NET PROFITS" APRIL 1995 PC PRO, pages 176,178-182, XP002059701 ISSN: 1355-4603 * left-hand column, line 181, last paragraph *	1-33	
A	BELLARE M ET AL: "IKP - A FAMILY OF SECURE ELECTRONIC PAYMENT PROTOCOLS" PROCEEDINGS OF THE FIRST USENIX WORKSHOP ON ELECTRONIC COMMERCE, JULY 11-12, 1995, pages 89-106, XP000579445 * page 95, right-hand column * * page 96, left-hand column, last paragraph *	1-33	
A	WO 96 00485 A (TELEFON AB LM ERICSSON) 4 January 1996 (1996-01-04) * page 6, line 1 - line 3; figure 1 * * page 7, line 32 - page 8, line 2 * * page 10, line 13 - page 11, line 29 *	1-33	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L G06F G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	5 July 2000	Vercauteren, S

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP___0813325A3_I_>

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 97 10 9412

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-07-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0590861 A	06-04-1994	CA 2100134 A	30-03-1994
		JP 7129671 A	19-05-1995
		MX 9305830 A	30-06-1994
		US 5485510 A	16-01-1996
WO 9600485 A	04-01-1996	US 5668876 A	16-09-1997
		AU 692881 B	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A	04-01-1996
		EP 0766902 A	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

BNSDOCID: <EP___0813325A3_I_>

THIS PAGE BLANK (USPTO)